Independent Verification and Validation (IV&V) – Adding Mission Assurance to NASA Flight Software

Shirley Savarino
TASC
1000 University Drive
Fairmont, WV 26554
304-368-3305
shirley.savarino@ivv.nasa.gov

Sanford Krasner
Jet Propulsion Laboratory
4800 Oak Grove Drive
Pasadena, CA
818-354-6612
sanford.krasner@jpl.gov

Frank Huy
NASA IV&V
1000 University Drive
Fairmont, WV 26554
304-367-8444
frank.a.huy@nasa.gov

Abstract—[1][2]

The NASA Independent Verification and Validation (IV&V) Facility objective is to identify potential defects in flight software using independent analysis techniques. This paper describes the tailored IV&V techniques that have been developed in support of critical interactions on the Mars Science Laboratory (MSL) project, scheduled to launch in November, 2011. The IV&V techniques for interface analysis use independently developed sequence diagrams of critical scenarios. The results from these analyses have had a positive impact on the requirements flow down, consistency amongst MSL requirements and identification of missing requirements. The results of these analyses and the positive impact to the MSL project are provided.

TABLE OF CONTENTS

1. INTRODUCTION

The NASA Independent Verification and Validation (IV&V) Facility works to identify potential defects in MSL flight software (FSW) artifacts utilizing independent analysis techniques. These techniques allow IV&V analysts to evaluate MSL FSW through full lifecycle development and result in technical issues which are provided to the MSL project for consideration.

IV&V analysis focuses on the most critical areas of MSL FSW which have been identified using the IV&V risk based analysis process. The MSL critical areas are entry, descent and landing (EDL), fault protection, sample acquisition/sample processing and handling (SA/SPaH) and autonomous surface operations (ASO). The MSL IV&V analysis uses a combination of standard and tailored techniques to ensure compliance to IV&V methods with appropriate tailoring to address MSL development processes, artifacts and the identified critical areas.

We describe a tailored IV&V technique that has been demonstrated on the MSL IV&V effort in support of the identified critical areas. The results of these analyses and impact to the MSL project are provided. Specifically, the IV&V techniques and results in the following are explored: Interface analysis using context diagrams and sequence diagrams of critical scenarios (using EDL as an example, with techniques extensible to surface operations)

MSL IV&V is enabled through a partnership between the MSL project and IV&V teams facilitated by the IV&V project manager, the MSL project software systems engineer and the IV&V contractor lead. This liaison is used to communicate activities on the mutual sides, and transfer MSL artifacts and IV&V findings. The liaison function balances the tension between IV&V wanting to get artifacts early and the project wanting IV&V findings to be reported on mature artifacts. This balance is established through the objective of timely and relevant IV&V findings.

The MSL project and IV&V project have negotiated particular maturity milestones for each artifact type. For example, flight software code is provided to IV&V upon the MSL system integration test delivery (vs. an early build integration test milestone). In selected cases, such as fault protection, early versions of artifacts are provided to aid in system understanding. MSL artifacts analyzed include SW requirements, Functional Design Descriptions, Software Descriptions Documents, code, V&V plans and procedures, and Interface Control Documents.

The results from these analyses have improved MSL requirements flow down, consistency amongst MSL requirements and identification of missing requirements. The significance of IV&V participation on the MSL project has resulted in early identification of software defects. Timely resolution of IV&V issues addresses these concerns and saves cost and schedule compared to finding these defects during testing or operation.

[1] IEEEAC paper#1290, Version 1, Updated 2011:01:11

[2] 978-1-4244-7351-9/11/$26.00 ©2011 IEEE

2. Adding Mission Assurance to NASA Flight Software

Selecting High Risk Software Capabilities for Analysis. The NASA Independent Verification and Validation (IV&V) Facility provides a mission assurance function to the NASA agency on the most critical software across NASA's space portfolio. Verification is the process of determining whether or not the software products of a given phase of the software design lifecycle (SDLC) fulfill the established requirements for that phase. Validation evaluates the software products throughout the SDLC to ensure those products meet the mission and customer's needs.

IV&V strives to maintain independence in three separate areas: technical independence, managerial independence, and financial independence. Technical independence is accomplished by independent review of project-developed artifacts. IVV analysts are not responsible for development of any artifacts, so they are isolated from "group think" or pride of ownership in the original design development.
Managerial and financial independence are maintained since the IVV facility is a separate NASA center, and is not funded by project funds. Additionally, IV&V independently selects which NASA Projects are analyzed.

Software IV&V is a systems engineering process employing rigorous methodologies for evaluating the correctness and quality of the software product throughout the SDLC. Software IV&V is adapted to the characteristics of the project. The objectives of NASA IV&V are described in NASA's SLP-09-01 [1].

IV&V uses risk based analysis methods to prioritize the effort to fit resources constraints using a process called the Probability Based Risk Analysis (PBRA). [2]. This method develops a risk matrix to prioritize mission capabilities to be analyzed. This risk matrix evaluates:

a.) the impact of failure or degradation of a particular mission capability,

b.) the likelihood of that failure.

The challenge is to develop a risk matrix to assess mission capabilities in order to prioritize the mission capabilities across the different NASA missions.

The IV&V PBRA process begins with an outline of the system capabilities, which represent the desired behaviors of the system to satisfy the goals of the mission. The capabilities are simply groups of related behaviors that achieve a mission goal. For the Mars Science Laboratory, the IV&V decomposition of the mission consists of the following capabilities:

- Launch Operations
- Cruise and Approach Operations
- Entry, Descent and Landing
- Surface Navigation
- Science Data Collection and Processing
- Ground Systems

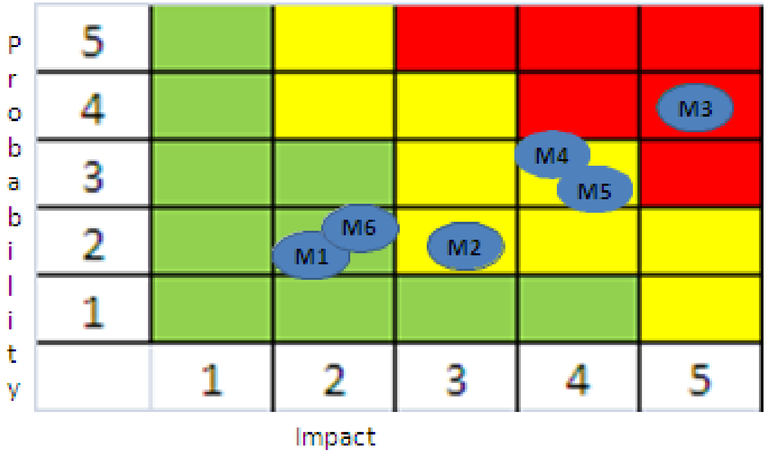
An impact assessment represents the relative importance of the capability itself. To determine importance, the effect a limitation or issue within the capability has on the overall mission is evaluated. The nature of the limitation for this assessment will more than likely be viewed as a limitation that fully prevents the capability from existing versus a limitation that simply degrades the capability. The purpose is to understand what the effect is if a limitation was to exist during operations. This analysis deals with the impact of the complete failure or absence of a capability. This is a simpler analysis than postulating possible degraded modes of operation.

The likelihood of a failure is represented by two components. The first component represents the likelihood that a limitation or issue will exist within the capability, including if appropriate degradations that might impact science collection but not harm the space assets or human life. The second component of likelihood represents the probability that this failure will occur during operations.

In summary, likelihood considers whether an artifact is likely to contain a defect and whether that defect is likely to impact implementation and operations. Impact considers whether the defect will impact the mission's science objectives, Level 1 requirements and human or asset safety.

The assessments result in a quantitative score, which can then be mapped into a 5x5 risk matrix. The color scheme for the matrix guides the amount of coverage IV&V provides per capability. Areas of the matrix shaded RED indicate FULL IV&V Coverage, areas shaded YELLOW indicate PARTIAL IV&V Coverage, and areas shaded GREEN indicate NO IV&V Coverage. Figure 1 illustrates the results of the risk assessment on the MSL mission.

The IV&V PBRA process was extended to elaborate on the YELLOW desired behaviors to achieve the stated parent capability to further establish scoping of PARTIAL IV&V coverage. This extension entailed a further decomposition of the capability and repeating the risk based assessment methodology on the results. The results and associated IV&V coverage were thus determined to be applied to the following MSL capabilities: The entry, descent and landing (EDL), fault protection, sample acquisition/sample processing and handling (SA/SPaH) and autonomous surface operations (ASO).



	MSL Risk Score Summary	Score	
	Capability	Impact	Prob
M1	MSL.Launch Operations	2	2.2
M2	MSL.Cruise and Approach Operations	3	2.4
M3	MSL.Entry Decent Landing	5	4.4
M4	MSL.Surface Navigation	4	3.2
M5	MSL.Science Data Collection & Processing	4	3.2
M6	MSL.Ground Operations	2	2.8

Figure 1: MSL IV&V Criticality Assessment Results

As an example of the type of analysis the IV&V performed on MSL and the nature of the IV&V's findings, a description of the work the IV&V performed on the MSL EDL capability is provided

Entry, Descent and Landing (EDL). EDL is ranked most critical in the MSL mission because it is: highly critical to mission success, fully autonomous and out of communications range with the ground team. EDL lasts approximately six minutes The criticality of EDL is high not only because of its impact, but also due to its likelihood (probability). EDL design on MSL is new, with no flight heritage.

Figure 2 illustrates the MSL EDL sequence [3]. The entry, descent, and landing (EDL) phase begins when the spacecraft reaches the martian atmosphere, about 125 kilometers (about 78 miles) above the surface, and ends with the rover safe and sound on the surface of Mars.

The sheer size of the Mars Science Laboratory rover (775 kilograms or over 1,700 pounds) would preclude it from taking advantage of an airbag-assisted landing. Instead, the Mars Science Laboratory will use the sky crane touchdown system, which will be capable of delivering a much larger rover onto the surface. It will place the rover on its wheels, ready to begin its mission.

The entry, descent and landing sequence consists of four parts:

- Guided Entry - The spacecraft will be controlled by small rockets during descent through the martian atmosphere, toward the surface.
- Parachute Descent - Like Viking, Pathfinder and the Mars Exploration Rovers, the Mars Science Laboratory will be slowed by a large parachute.
- Powered Descent - Again, rockets will control the spacecraft's descent until the rover separates from its final delivery system, the sky crane.

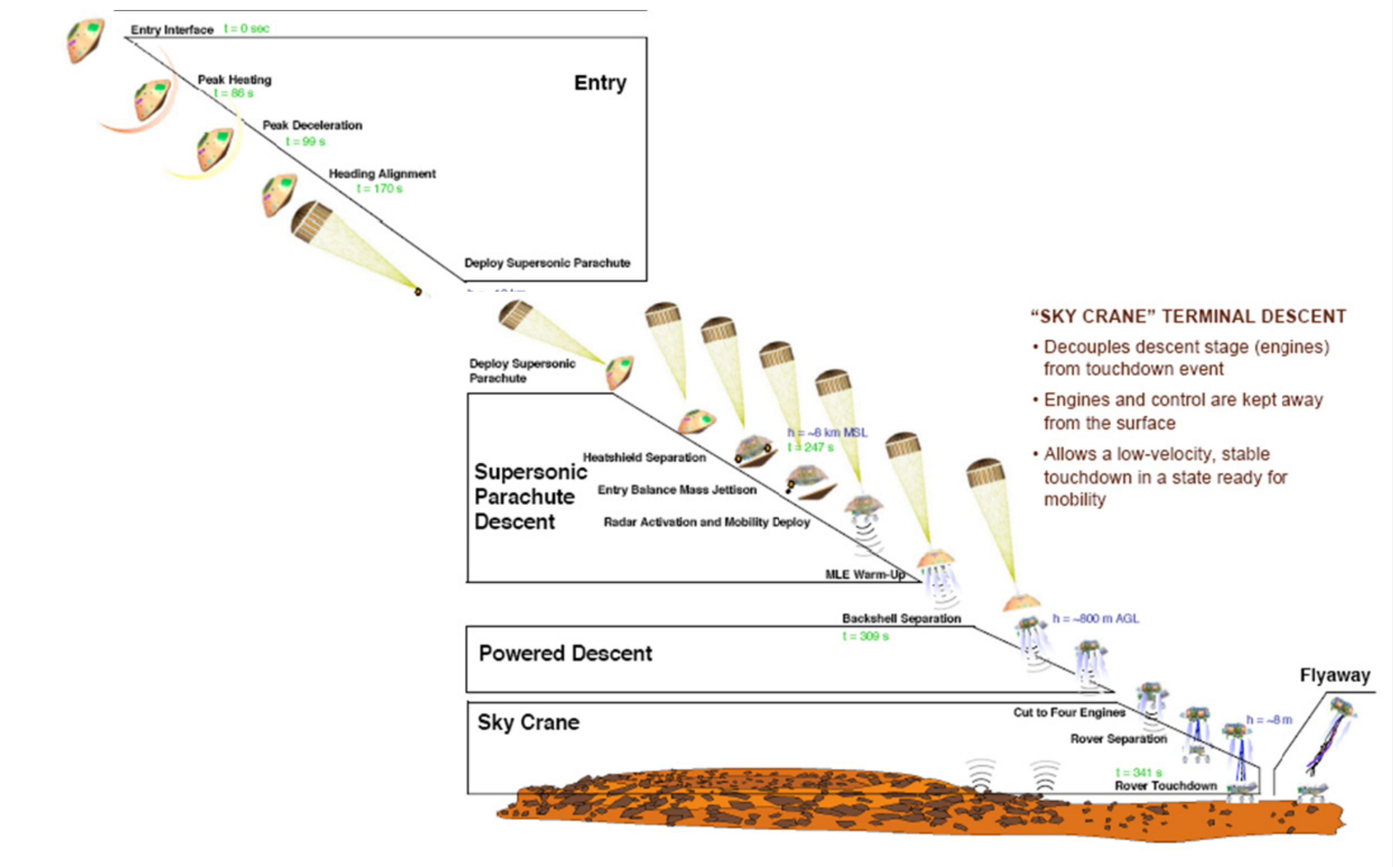

Entry Interface t = 0 sec
Peak Heating t = 86 s
Peak Deceleration t = 99 s
Heading Alignment t = 170 s
Entry
Deploy Supersonic Parachute
Deploy Supersonic Parachute
"SKY CRANE" TERMINAL DESCENT
• Decouples descent stage (engines) from touchdown event
• Engines and control are kept away from the surface
• Allows a low-velocity, stable touchdown in a state ready for mobility
h = ~8 km MSL
t = 247 s
Heatshield Separation
Supersonic Parachute Descent
Entry Balance Mass Jettison
Radar Activation and Mobility Deploy
MLE Warm-Up
Backshell Separation
t = 309 s
h = ~800 m AGL
Powered Descent
Flyaway
Sky Crane
Cut to Four Engines
Rover Separation
h = ~8 m
t = 341 s
Rover Touchdown

Figure 2: MSL EDL Sequence

- Sky Crane - Like a large crane on Earth, the sky crane system will lower the rover to a "soft landing"-wheels down - on the surface of Mars.

Several IV&V analyses were performed on the MSL EDL capability, including correlation between the requirements, design and timeline, interface analysis. Interface analysis is detailed as an example of IV&V findings.

Interface Analysis..The objective behind the IV&V interface analysis was to provide additional assurance that devices are used appropriately during EDL. In particular, device use is compared to constraints specified in Interface Control Documents (ICDs) or other documents. During various EDL phases, the number of devices that the EDL timeline must interface with varies from about a dozen to over thirty. The operations and timing use and constraints that needed to be adhered to were understood through reading the device specifications. It was assumed that the device specifications provided the correct usage and operational constraints that would need to be adhered to in the EDL timeline.

The MSL IV&V team assessed the EDL activities based on the number of devices interacting with the timeline and the associated criticality of operations and chose to perform interface scenario based analysis on the following two scenarios:

- Cruise – EDL Transition
- Powered Descent and Sky Crane Operations

There are three steps in the Interface Analysis: Device understanding, Mapping of associated requirements to the Timeline, and Device Operation within the Timeline. Each of these steps are described in the following sections.

Device understanding; services expected and provided. The first step in the analysis process is to identify and understand the devices that operate as part of the associated scenario. There were 34 devices associated with the cruise-EDL transition sequence and 17 devices associated with the powered descent and sky crane operations. Next, services anticipated and received were envisioned per device.

A list of the potential device services is provided in Table 1.

Communication Mechanism (e. g. 1553, direct connection)
Device power states (On, Off, Unknown, Boot up, Initialization)
State definition and transitions
Thresholds (signals, data)
Data obtained from device (e.g. star info from star trackers)
Reporting mechanism
Commands and Telemetry
Redundancy
Timing usage constraints
Monitors (Health Status and Fault)

Table 1. Device Services

This task was performed using multiple MSL artifacts associated with EDL. The decomposition of capability in the functional description documents (FDDs) was centered with the timeline in one FDD. However, the devices that supported EDL were described in other documents. There was an FDD that described EDL sensors and another that described EDL actuators. A separate FDD described the cruise phase actuators and sensors. The benefit of this task was the identification of requirements and device operation constraints that needed to be met in the construction of the EDL timeline.

Mapping of associated requirements to the Timeline. Requirements identified from the "services provided/expected" exercise were then added to the EDL timeline provided by the MSL project. The provided timeline included time anchors, specific actions that occurred within an anchor and an action description. Each action also had associated timestamps relative to EDL entry. IV&V augmented the provided timeline with the information obtained through the "services" step, and mapped device operation/constraint requirements and design against each EDL action step, as applicable. An example of the requirements mapping is shown in Figure 3.

The IV&V activities actually occurred in three passes. The first pass was to add information to the provided timeline that focused on the devices required to support a timeline action (see pass 1 in Figure 3). The second pass computed elapsed time between activities and brought in the requirements associated from the device services. These requirements would primarily come from the supporting EDL FDDs such as the sensors, actuators and cruise FDD descriptions of device operations (see pass 2 of Figure 3). The final step was to assess the data from pass 1 and 2 to determine if there were any violations in how the device was supposed to be used during EDL compared to how the device was actually implemented in the timeline.

Device Operation within the Timeline. The final step of the modeling/independent analysis consisted of "pivoting" information in the prior step. The pivoting transformed the view from the sequence of events to a device centric view mapped against time. The model view included:

- Use of color in the device model view indicated various device states (on, off, idle, in-process).
- Summary of the start and end states associated with each device

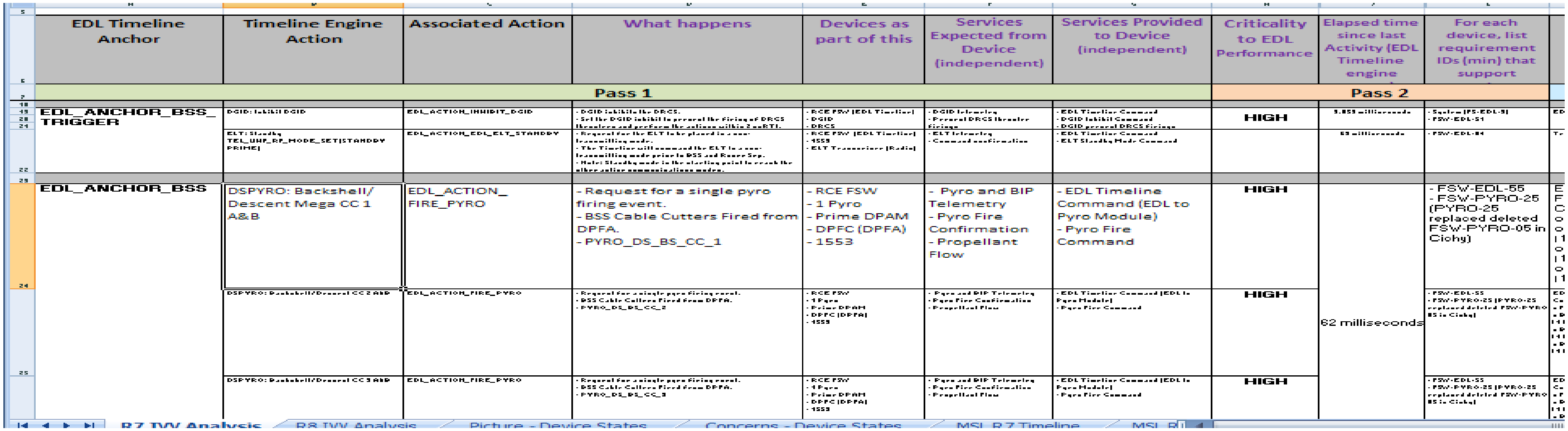
This view allowed IV&V to readily analyze the operation of any given device during EDL. The actual device operation could then be compared to expected operation of the device which was defined in the services step. Figure 4 shows an example of the device centric view.

Results to the MSL project. The analysis proved useful in analyzing device use during the complex EDL timeline. The EDL timeline had between 20-30 devices that needed to be orchestrated in concert with the actual algorithms performing EDL. The time criticality and importance of this capability to the MSL mission as well as the distributed nature of the specifications (often, the device requirements and design were provided in a different artifact than the timeline itself) compelled new IV&V analysis techniques. All findings from this analysis were discussed with the MSL project and addressed in a subsequent release of the EDL specification.

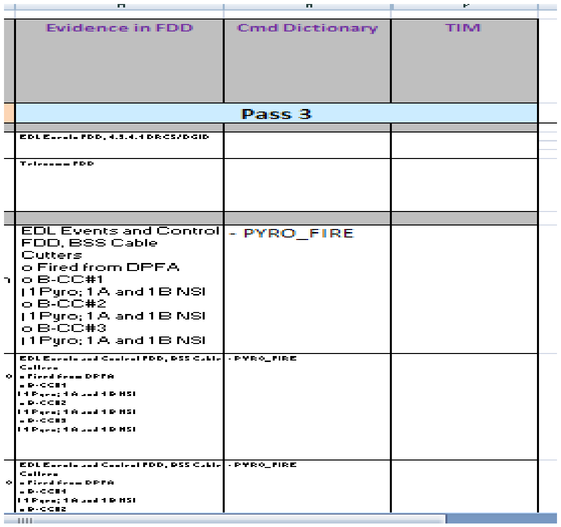
This analysis yielded the following types of findings:

- Potential timing violations: device specification would describe timing requirements which were not followed in the timeline (e.g. turn on the radar by a certain time),
- Incomplete implementation of modes of operation: the stated device modes were not completely implemented in the timeline
- Conflicts in device usage (e.g. requirements indicating that devices should not be simultaneously on, while timeline showed warmup of one device during operation of the other).

The MSL project has stated that the analyses performed by IV&V across multiple artifacts were especially beneficial to add assurance to the development. IV&V has recognized that the modeling techniques used in this analysis facilitated understanding of the EDL sequence and enhanced findings provided.



EDL Timeline Anchor	Timeline Engine Action	Associated Action	What happens	Devices as part of this	Services Expected from Device (independent)	Services Provided to Device (independent)	Criticality to EDL Performance	Elapsed time since last Activity (EDL Timeline engine	For each device, list requirement IDs (min) that support	
Pass 1							Pass 2			
EDL_ANCHOR_BSS_TRIGGER	DGID: Inhibit DGID	EDL_ACTION_INHIBIT_DGID	- DGID inhibits the DRCS. - Set the DGID inhibit to prevent the firing of DRCS thrusters and perform the actions within 2 msRTI.	- RCE FSW (EDL Timeline) - DGID - DRCS	- DGID telemetry - Prevent DRCS thruster firings	- EDL Timeline Command - DGID Inhibit Command - DGID prevent DRCS firings	HIGH	1.853 milliseconds	- System (FS-EDL-5) - FSW-EDL-51	ED
	ELT: Standby TEL_UHF_RF_MODE_SET(STANDBY PRIME)	EDL_ACTION_EDL_ELT_STANDBY	- Request for the ELT to be placed in a non-transmitting mode. - The Timeline will command the ELT to a non-transmitting mode prior to BSS and Rover Sep. - Note: Standby mode is the starting point to reach the other active communications modes.	- RCE FSW (EDL Timeline) - 1553 - ELT Transceiver (Radio)	- ELT telemetry - Command confirmation	- EDL Timeline Command - ELT Standby Mode Command		53 milliseconds	- FSW-EDL-84	Tr
EDL_ANCHOR_BSS	DSPYRO: Backshell/ Descent Mega CC 1 A&B	EDL_ACTION_ FIRE_PYRO	- Request for a single pyro firing event. - BSS Cable Cutters Fired from DPFA. - PYRO_DS_BS_CC_1	- RCE FSW - 1 Pyro - Prime DPAM - DPFC (DPFA) - 1553	- Pyro and BIP Telemetry - Pyro Fire Confirmation - Propellant Flow	- EDL Timeline Command (EDL to Pyro Module) - Pyro Fire Command	HIGH	62 milliseconds	- FSW-EDL-55 - FSW-PYRO-25 (PYRO-25 replaced deleted FSW-PYRO-05 in Cichy)	E F C o o |1 o |1 o |1
	DSPYRO: Backshell/Descent CC 2 A&B	EDL_ACTION_FIRE_PYRO	- Request for a single pyro firing event. - BSS Cable Cutters Fired from DPFA. - PYRO_DS_BS_CC_2	- RCE FSW - 1 Pyro - Prime DPAM - DPFC (DPFA) - 1553	- Pyro and BIP Telemetry - Pyro Fire Confirmation - Propellant Flow	- EDL Timeline Command (EDL to Pyro Module) - Pyro Fire Command	HIGH		- FSW-EDL-55 - FSW-PYRO-25 (PYRO-25 replaced deleted FSW-PYRO-05 in Cichy)	ED Co
	DSPYRO: Backshell/Descent CC 3 A&B	EDL_ACTION_FIRE_PYRO	- Request for a single pyro firing event. - BSS Cable Cutters Fired from DPFA. - PYRO_DS_BS_CC_3	- RCE FSW - 1 Pyro - Prime DPAM - DPFC (DPFA) - 1553	- Pyro and BIP Telemetry - Pyro Fire Confirmation - Propellant Flow	- EDL Timeline Command (EDL to Pyro Module) - Pyro Fire Command	HIGH		- FSW-EDL-55 - FSW-PYRO-25 (PYRO-25 replaced deleted FSW-PYRO-05 in Cichy)	ED Co

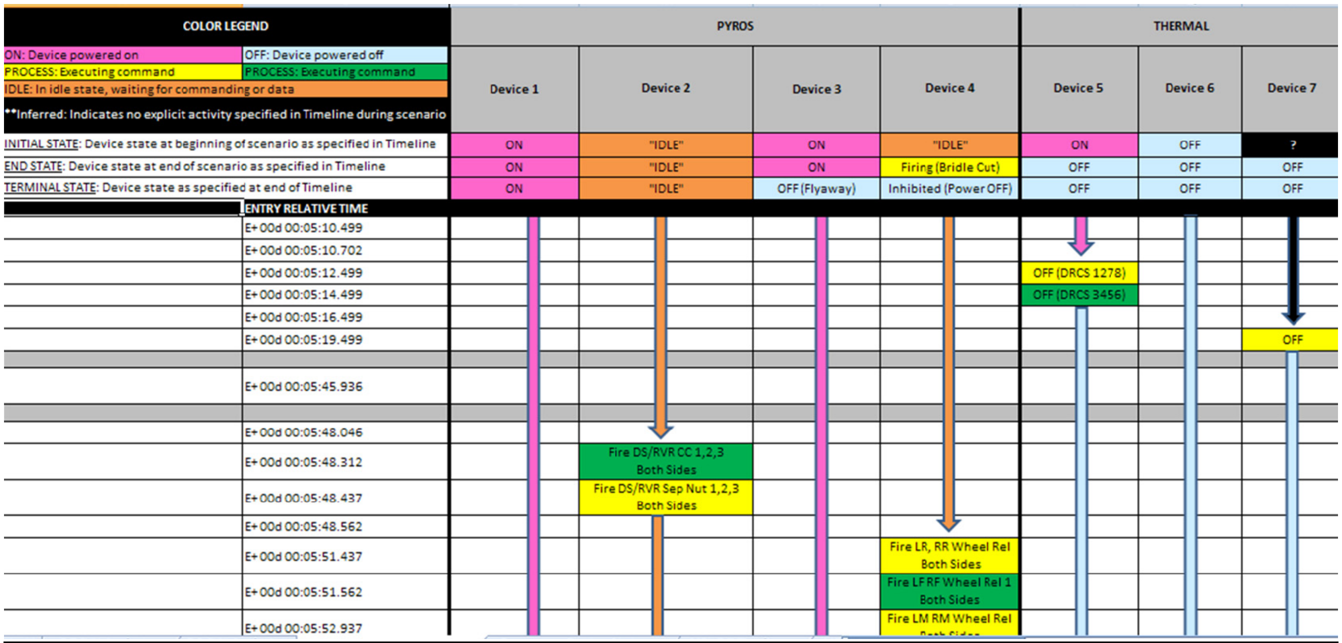


Evidence in FDD	Cmd Dictionary	TIM
Pass 3		
EDL Events FDD, 4.3.4.1 DRCS/DGID		
Telecomm FDD		
EDL Events and Control FDD, BSS Cable Cutters o Fired from DPFA o B-CC#1 | 1 Pyro; 1 A and 1 B NSI o B-CC#2 | 1 Pyro; 1 A and 1 B NSI o B-CC#3 | 1 Pyro; 1 A and 1 B NSI	- PYRO_FIRE	
EDL Events and Control FDD, BSS Cable Cutters o Fired from DPFA o B-CC#1 | 1 Pyro; 1 A and 1 B NSI o B-CC#2 | 1 Pyro; 1 A and 1 B NSI o B-CC#3 | 1 Pyro; 1 A and 1 B NSI	- PYRO_FIRE	
EDL Events and Control FDD, BSS Cable Cutters o Fired from DPFA o B-CC#1 | 1 Pyro; 1 A and 1 B NSI o B-CC#2	- PYRO_FIRE	

IV&V Analysis Notes:

- Columns in “black” come directly from the EDL Timeline
- Columns in “purple” are IV&V derived or extracted information from other MSL related sources
- The analysis was performed in three passes (indicated via Pass 1, Pass 2, and Pass 3)
- Timepoint information associated with firing one of the descent pyros to support backshell separation is enlarged as an example for discussion

Figure 3: Requirements/Design mapped to Sequence View



COLOR LEGEND

ON: Device powered on | OFF: Device powered off

PROCESS: Executing command | PROCESS: Executing command

IDLE: In idle state, waiting for commanding or data

**Inferred: Indicates no explicit activity specified in Timeline during scenario

		PYROS				THERMAL		
		Device 1	Device 2	Device 3	Device 4	Device 5	Device 6	Device 7
INITIAL STATE: Device state at beginning of scenario as specified in Timeline		ON	"IDLE"	ON	"IDLE"	ON	OFF	?
END STATE: Device state at end of scenario as specified in Timeline		ON	"IDLE"	ON	Firing (Bridle Cut)	OFF	OFF	OFF
TERMINAL STATE: Device state as specified at end of Timeline		ON	"IDLE"	OFF (Flyaway)	Inhibited (Power OFF)	OFF	OFF	OFF
	ENTRY RELATIVE TIME							
	E+00d 00:05:10.499							
	E+00d 00:05:10.702							
	E+00d 00:05:12.499					OFF (DRCS 1278)		
	E+00d 00:05:14.499					OFF (DRCS 3456)		
	E+00d 00:05:16.499							
	E+00d 00:05:19.499							OFF
	E+00d 00:05:45.936							
	E+00d 00:05:48.046							
	E+00d 00:05:48.312		Fire DS/RVR CC 1,2,3 Both Sides					
	E+00d 00:05:48.437		Fire DS/RVR Sep Nut 1,2,3 Both Sides					
	E+00d 00:05:48.562							
	E+00d 00:05:51.437				Fire LR, RR Wheel Rel Both Sides			
	E+00d 00:05:51.562				Fire LF RF Wheel Rel 1 Both Sides			
	E+00d 00:05:52.937				Fire LM RM Wheel Rel			

Figure 4: Device Centric View of EDL Sequence

Benefits of this analysis to the IV&V Program. The IV&V program utilizes a catalog of methods which contains IV&V analyses techniques. The Catalog forms the basis for an engineered approach to achieving the desired level of software assurance on Mission Projects for which IV&V is required and authorized. Methods in the Catalog support one or more Goals of IV&V as defined in System Level Procedure (SLP) 09-1, "Independent Verification and Validation Technical Framework." The Catalog defines the set of Methods approved for implementation on IV&V Projects, and embodies lessons learned and best practices in applying those Methods productively.

New Methods can be added to the Catalog as needed. New Methods can be suggested by experience, relevant technology or advances from other related fields, result from on-going research and development, by new technologies and tools, or it could simply be the documentation of a tried-and-true Method that has not, as yet, been documented and included in the Catalog.

The MSL IV&V interface analysis and correlation have been briefed at IV&V technical meetings for knowledge sharing and are targeted to be added to the IV&V Catalog of Methods.

Other MSL techniques that were used to analyze high risk capabilities. The primary focus areas for the IV&V analyses based on criticality have been EDL and MSL fault protection. In addition to the interface analyses described in this paper, IV&V has performed the following tasks:

- Correlation analysis between the EDL timeline (which is ultimately autocoded into the MSL code itself), requirements, action tables
- EDL timeline fault protection analysis
- Timing constraints, allocations, and actual implementation of actions within the timeline

The MSL fault protection was not identified as a separate capability since it operates during all mission phases. The highly autonomous nature of an interplanetary mission leaves little to no time for ground intervention during faults. The MSL spacecraft must be able to ensure its own safety autonomously. Some challenges faced by MSL fault protection include:

- If the MSL rover experienced a failure during a drilling operation, it cannot just halt. A halt might mean that the drill could not be extracted from the Martian rock at a later time.
- How to address “simultaneous failures” within the MSL spacecraft and ensuring that fault responses don’t contradict each other.

To support MSL fault protection, IV&V did a consistency audit across the subsystems. This audit entailed ensuring that all fault monitors had an accompanying requirement. Additionally the audit entailed that all fault monitors (which numbered over 1000) anticipated by the system fault protection were implemented in the flight software.

MSL Lines of Communication.

Technical rigor of the IV&V analysis performed is established through a thorough understanding of the MSL development process and associated artifacts. The understanding is facilitated through bi-weekly teleconferences, IV&V attendance at MSL project reviews and face-to-face meetings which occur approximately on a bimonthly basis.

Benefits of the lines of communication used on the MSL IV&V interactions include

- Mutual understanding of activities, leading to "no-surprises"
- Assurance that artifacts are of the appropriate maturity for IV&V analysis

Technical rigor in IV&V methods that is appropriate to the criticality of the MSL capability and optimized for effectiveness.

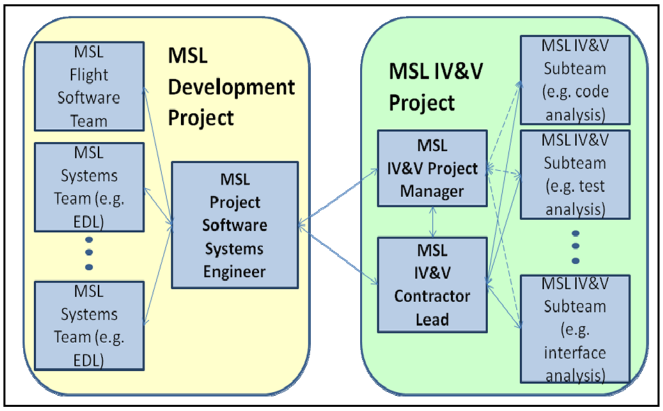

MSL Flight Software Team
MSL Systems Team (e.g. EDL)
MSL Systems Team (e.g. EDL)
MSL Development Project
MSL Project Software Systems Engineer
MSL IV&V Project
MSL IV&V Project Manager
MSL IV&V Contractor Lead
MSL IV&V Subteam (e.g. code analysis)
MSL IV&V Subteam (e.g. test analysis)
MSL IV&V Subteam (e.g. interface analysis)

Figure 5: MSL Lines of Communication

3. Conclusions

The MSL IV&V effort adds value to the MSL project and the IV&V program through a series of activities, including:

- Identification of critical areas of analysis using a risk based approach,
- An IV&V Catalog of Methods which provide a basis for performing IV&V analyses,
- Analysis techniques that are appropriate to the MSL project,
- Open lines of communication between the MSL project and IV&V effort, and
- Incorporation of the MSL based tailored analyses back into the IV&V catalog of methods for use on future IV&V efforts.

Benefits of the IV&V effort have resulted in additional confidence in the correct implementation of the software associated with the MSL mission.

References

[1] NASA SLP 09-01 on the NASA I&V System Level Procedures and Work Instructions Website, http://www.nasa.gov/centers/ivv/ims/slps/index.html

[2] Kurt Woodham, Tom Marshall, Steve Driskell, and Marcus Fisher, "Risk Matrix to Support the IV&V Program Portfolio, Version 9", September 3, 2008.

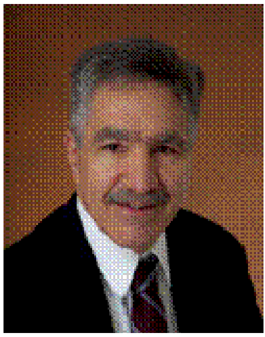
[3] Mars Science Laboratory Web site http://marsprogram.jpl.nasa.gov/msl/

[4]NASA's 2009 Mars Science Laboratory Overview, MSL Project, Jet Propulsion Laboratory, California Institute of Technology http://marsoweb.nas.nasa.gov/landingsites/msl/memoranda/MSL_overview_LS.pdf

.

Biography

Shirley Savarino *has worked on Independent Verification and Validation of Space Science, Planetary and Manned NASA missions for the past 7 years She is currently the contractor lead for the IV&V efforts associated with the Mars Science Laboratory. Prior to her IV&V activities, she worked in satellite development for 15 years. She has led the Concept of Operations for an operational weather satellite and worked in satellite development at TRW. She has a BSME from MIT and an MSEE from USC.*



Sanford Krasner *specializes in system design and integration of planetary mission software. He has worked on Galileo, Cassini, Mars Observer and Deep Space 1 missions. He is currently the Project Software System Engineer for the Mars Science Laboratory project. In this role, he is the project point-of-contact for the NASA IV&V facility.*

Frank Huy *has been an IV&V project manager for NASA for the last 10 years. His current position is as the project manager for the Mars Science Laboratory and the Soil Moisture Active & Passive projects. Prior projects Frank has managed include the James Web Space Telescope, Orion, Galex and the Hubble Space Telescope. He has also held positions as the Goddard and Applied Physics Center Lead, and the IV&V Modeling and Validation Lead. Prior to working for the Government, he worked at Rockwell Autonetics on the B1 Bomber. He has a BSEE from WVU.*

ACKNOWLEDGEMENTS

Special acknowledgement is extended to Paula Baker and Dustin Whitt who are members of the IV&V MSL team and participated in the EDL interface analysis activities.

The work described in this paper was carried out by the NASA IV&V Facility and supported by the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.